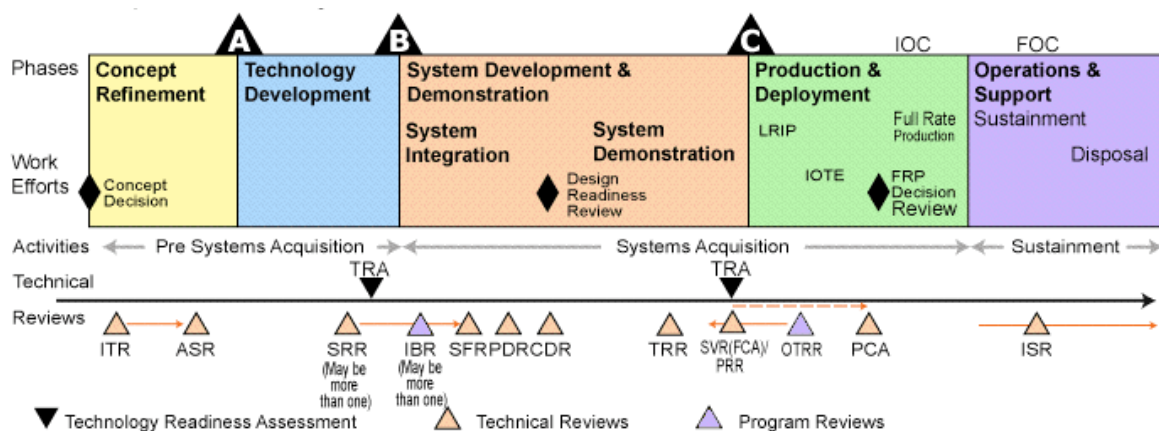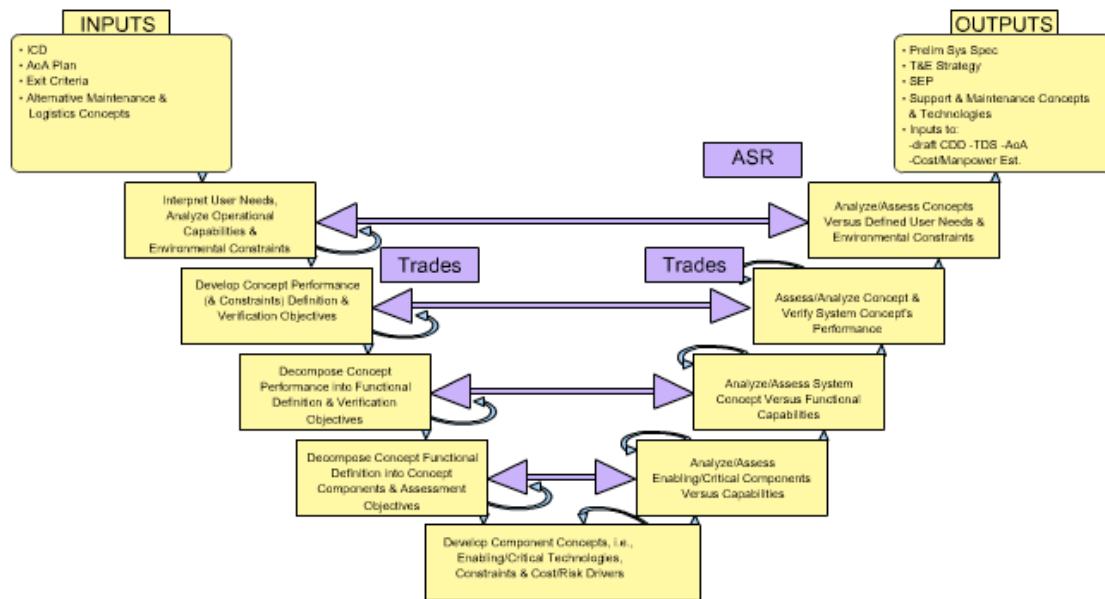# System Safety in Systems Engineering V-Charts

System Safety is an integral part of the systems engineering (SE) process, providing specific inputs by activity and phase as illustrated in the five V-Charts - one for each phase of the system's life cycle. Following each V-Chart is a list of the systems engineering steps and technical reviews and the corresponding system safety activities that are completed during that phase.

Concept Refinement Phase

Concept Refinement Phase V-Chart

INPUTS
- ICD
- AoA Plan
- Exit Criteria
- Alternative Maintenance & Logistics Concepts

OUTPUTS
- Prelim Sys Spec
- T&E Strategy
- SEP
- Support & Maintenance Concepts & Technologies
- Inputs to:
  - draft CDD -TDS -AoA
  - -Cost/Manpower Est.

ASR

Interpret User Needs, Analyze Operational Capabilities & Environmental Constraints

Analyze/Assess Concepts Versus Defined User Needs & Environmental Constraints

Trades

Trades

Develop Concept Performance (& Constraints) Definition & Verification Objectives

Assess/Analyze Concept & Verify System Concept's Performance

Decompose Concept Performance into Functional Definition & Verification Objectives

Analyze/Assess System Concept Versus Functional Capabilities

Decompose Concept Functional Definition into Concept Components & Assessment Objectives

Analyze/Assess Enabling/Critical Components Versus Capabilities

Develop Component Concepts, i.e., Enabling/Critical Technologies, Constraints & Cost/Risk Drivers

Inputs	System Safety Should:
Initial Capabilities Document (ICD)	Provide inputs as requested
Analysis of Alternatives (AoA) Plan	Participate in AoA development
Exit Criteria	Provide the following exit criteria: 1. Preliminary Hazard List (PHL) 2. Strategy for integrating Environment, Safety, and Occupational Health (ESOH) risk management into the Systems Engineering Plan (SEP)
Alternative Maintenance and Logistics Concepts	Provide inputs as requested

Interpret User Needs, Analyze Operational Capabilities & Environmental Constraints

System Safety should:
1. Review System Threat Assessment
2. Identify applicable system safety ESOH criteria

Develop Concept Performance (& Constraints) Definition & Verification Objectives

System Safety should assess each system concept against identified system safety criteria.

Concept Refinement Phase

Decompose Concept Performance into Functional Definition & Verification Objectives

System Safety should:

1. Translate concept-level system safety criteria into functional requirements
2. Identify applicable verification objectives

Decompose Concept Functional Definition into Concept Components & Assessment Objectives

System Safety should:

1. Initiate PHL
2. Review historical information (e.g., successes, mishaps, lessons-learned)

Develop Component Concepts, i.e., Enabling/Critical Technologies, Constraints & Cost/Risk Drivers

System Safety should:

1. Update PHL
2. Initiate identification of component constraints
3. Recommend input into projected system attrition rates

Analyze/Assess Enabling/Critical Components Versus Capabilities

System Safety should:
1. Identify safety requirements against critical component capabilities
2. Evaluate component test results against identified system constraints.

Analyze/Assess System Concept Versus Functional Capabilities

System Safety should evaluate system safety functional requirements for the system concept based upon component test results.

Assess/Analyze Concept & Verify System Concept's Performance

System Safety should evaluate system concept's ability to meet performance capability requirements within identified safety constraints.

Analyze/Assess Concepts Versus Defined User Needs & Environmental Constraints

System Safety should:

1. Finalize PHL for each system concept
2. Recommend preferred approach for system concept

Alternative Systems Review (ASR)

System Safety should:

1. Prepare results of PHL for each alternative
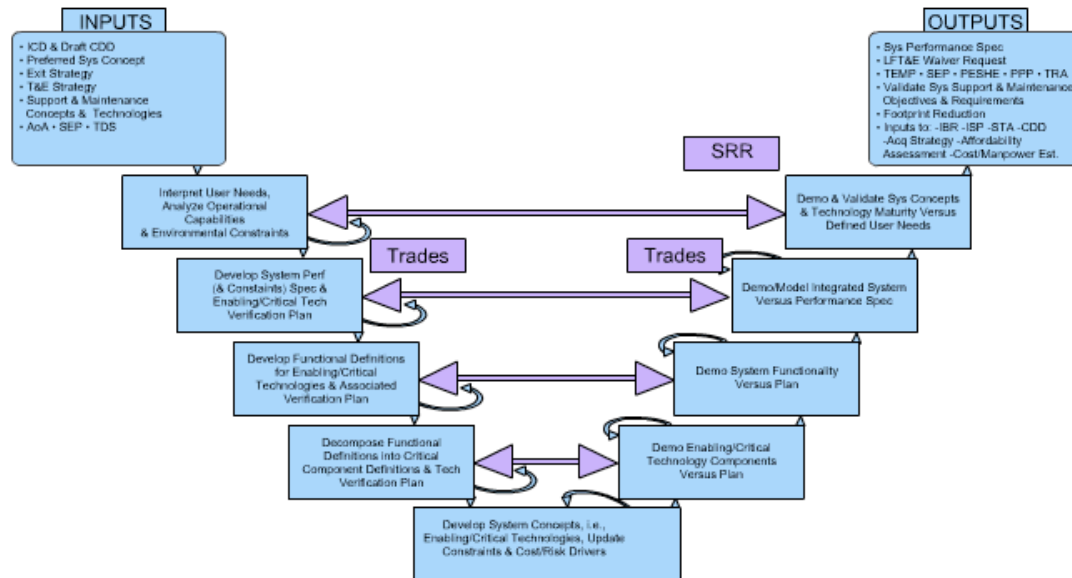2. Recommend System Safety level of effort required for the Technology phase

Trades

Throughout this phase, System Safety should participate in the trade studies to identify potential top-level hazards and ensure safety evaluation factors are included in the trade studies.

Concept Refinement Phase

Outputs	System Safety Should:
Preliminary System Specification	1. Provide PHL 2. Provide system safety criteria
Test and Evaluation (T&E) Strategy	1. Provide hazard risk mitigation test and verification methodologies 2. Provide approach towards obtaining safety release(s)
Systems Engineering Plan (SEP)	Participate in developing the strategy for integrating ESOH risk management
Support and Maintenance Concepts and Technologies	1. Identify potential ESOH operations and maintenance issues 2. Identify emerging system safety technologies 3. Identify emerging technology hazards

Technology Development Phase

Technology Development Phase V-Chart

Inputs	System Safety Should:
Initial Capabilities Document (ICD) and Draft Capability Development Document (CDD)	Develop system safety criteria and requirements
Preferred System Concept	Evaluate system concept against identified system safety criteria
Exit Criteria	Provide the following exit criteria: 1. Update Preliminary Hazard List (PHL) 2. Update strategy for integrating Environment, Safety, and Occupational Health (ESOH) risk management into systems engineering (SE)
Test and Evaluation (T&E) Strategy	1. Incorporate hazard risk mitigation test and verification methodologies 2. Provide approach toward obtaining safety release(s)
Support and Maintenance Concepts and Technologies	Provide inputs as requested
Analysis of Alternatives (AoA)	Characterize ESOH footprints or risks for AoA development
Systems Engineering Plan (SEP)	Update strategy for integrating ESOH risk management into SE
Technology Development Strategy (TDS)	1. Include strategy to identify hazards 2. Identify needed ESOH technology development

Technology Development Phase

Interpret User Needs, Analyze Operational Capabilities & Environmental Constraints

System Safety should:
1. Update identification of system safety constraints
2. Develop safety criteria
3. Identify ESOH-critical technology needs

Develop System Performance (& Constraints) Specifications & Enabling/Critical Technologies and Verification Plan

System Safety should:
1. Update system safety criteria
2. Include system safety-critical specifications in Verification Plan

Develop Functional Definitions for Enabling/Critical Technologies & Associated Verification Plan

System Safety should:
1. Update system safety criteria
2. Develop requirements for verification of risk mitigation controls

Decompose Functional Definitions into Critical Component Definition & Technologies Verification Plan

System Safety should:
1. Update system safety criteria
2. Develop requirements for verification of component risk mitigation controls

Develop System Concepts, i.e., Enabling/Critical Technologies, Update Constraints & Cost/Risk Drivers

System Safety should:
1. Update PHL
2. Update constraints
3. Identify potential operational and maintenance training and staffing requirements
4. Refine input for system attrition rates

Demo Enabling/Critical Technology Components Versus Plan

System Safety should:
1. Evaluate enabling/critical technologies from a system safety perspective
2. Review demo results for new technology component hazards

Demo System Functionality Versus Plan

System Safety should:
1. Evaluate enabling/critical technologies from a system safety perspective
2. Review demo results for new hazards

Demo/Model Integrated System Versus Performance Specifications

System Safety should:
1. Evaluate enabling/critical technologies from a system safety perspective
2. Review demo/model results for hazards

Technology Development Phase

Demo and Validate System Concepts & Technology Maturity Versus Defined User Needs

System Safety should:
1. Evaluate enabling/critical technologies from a system safety perspective
2. Review demo/validate model results for hazards

System Requirements Review (SRR)

System Safety should prepare and present system safety performance criteria at SRR.

Trades

Throughout this phase, System Safety should participate in the trade studies to evaluate options against identified system safety criteria.
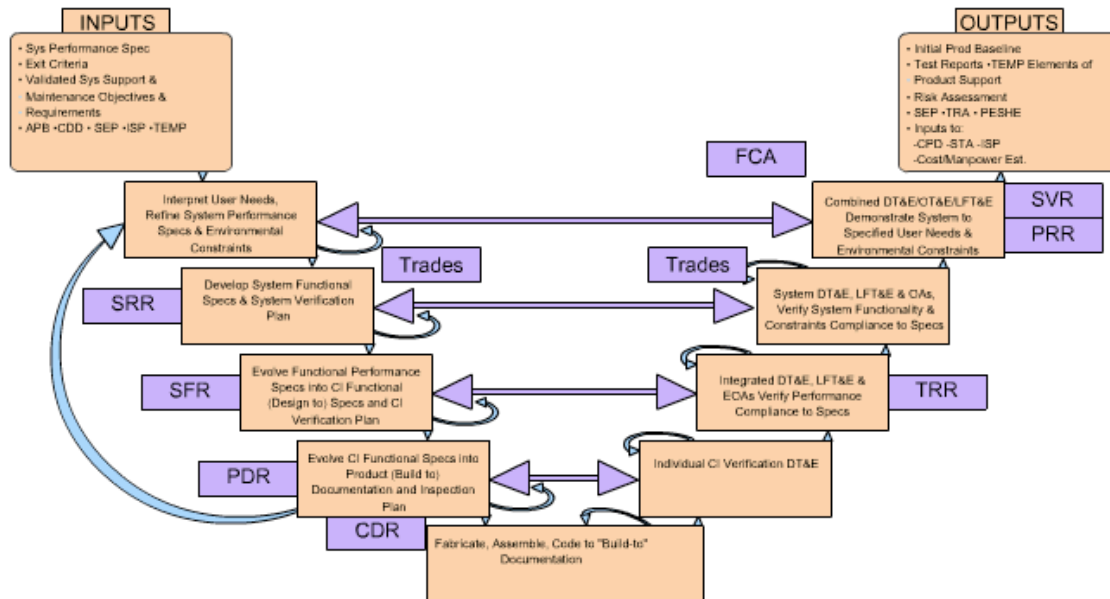
Outputs	System Safety Should:
System Performance Specification	1. Include Safety Requirements/Criteria Analysis (SRCA) data 2. Require concurrence/approvals from the applicable safety boards 3. Include applicable specifications (e.g., MIL-STD-2105C, MIL-STD-1316, MIL-STD-331, MIL-STD-1901, MIL-STD-464, IEEE/EIA 12207, HAZMAT list to avoid, 29CFR1910.95)
Live Fire Test and Evaluation (LFT&E) Waiver Request	1. Evaluate risk implications for not doing LFT&E 2. Develop proposed alternative approach for system survivability verification, e.g., subscale live fire test
Test and Evaluation Master Plan (TEMP)	1. Document specific test requirements (e.g., MIL-STD-2105C, MIL-STD-1316, MIL-STD-331, MIL-STD-1901, MIL-STD-464, IEEE/EIA 12207, HAZMAT list to avoid, 29CFR1910.95) 2. Identify requirements for verification of risk mitigation controls (based on system safety analyses) 3. Identify safety release requirements, e.g., SAR
Systems Engineering Plan (SEP)	1. Update strategy for integrating ESOH risk management into SE 2. Identify applicable safety boards and process for concurrence/approval
Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE)	1. Identify hazards 2. Include hazard analyses 3. Identify applicable safety boards and process for concurrence/approval
Program Protection Plan (PPP)	Provide inputs as requested
Technology Readiness Assessment (TRA)	Update risk mitigation technology readiness levels (e.g., insensitive munitions technology)

Technology Development Phase

Outputs	System Safety Should:
Validated System Support and Maintenance Objectives and Requirements	Provide preliminary requirements for system support and maintenance
Footprint Reduction	Provide ESOH input
Inputs to: • Integrated Baseline Review (IBR)	Provide inputs as requested
• Integrated Support Plan (ISP)	Provide inputs as requested
• System Threat Assessment (STA)	Provide inputs as requested
• Capability Development Document (CDD)	1. Provide hazard mitigation requirements 2. Provide insensitive munitions requirements 3. Provide mishap reduction requirements
• Acquisition Strategy	1. Summarize PESHE 2. Recommend incentives for enhancing system safety 3. Recommend incentives for ensuring a robust system safety effort as a key SE element
• Affordability Assessment	Provide inputs as requested
• Cost/Manpower Estimate	1. Recommend operations and maintenance training and staffing requirements 2. Update mishap reduction requirements

System Development and Demonstration Phase

System Development and Demonstration Phase V-Chart

Inputs	System Safety Should:
System Performance Specification	1. Include the Safety Requirements/Criteria Requirements Analysis (SRCA) data 2. Include applicable specifications (e.g., MIL-STD-2105C, MIL-STD-1316, MIL-STD-331, MIL-STD-1901, MIL-STD-464, IEEE/EIA 12207, HAZMAT list to avoid, 29CFR1910)
Exit Criteria	1. Document risk disposition of identified hazards, e.g., Safety Assessment Report (SAR) 2. Obtain concurrence/approval of appropriate safety boards 3. Update Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE)
Validated System Support and Maintenance Objectives & Requirements	Identify operating, maintenance, and support hazards
Acquisition Program Baseline	Provide inputs as requested
Capability Development Document (CDD)	1. Identify hazard mitigation requirements (e.g., electromagnetic environmental effects) 2. Identify insensitive munitions requirements 3. Identify mishap reduction requirements

System Development and Demonstration Phase

Inputs	System Safety Should:
Systems Engineering Plan (SEP)	1. Update strategy for integrating ESOH risk management into SE (e.g., Integrated Product Team (IPT) Process, technical reviews, etc.) 2. Identify applicable safety boards and process for concurrence/approval
Integrated Support Plan (ISP)	Provide guidance on performance feedback and hazard communication
Test and Evaluation Master Plan (TEMP)	1. Identify specific test requirements (e.g., MIL-STD-2105C, MIL-STD-1316, MIL-STD-331, MIL-STD-1901, IEEE/EIA 12207, 29CFR1910) 2. Identify requirements for verification of risk mitigation controls (based upon system safety analyses) 3. Identify safety release requirements, e.g., SAR

Interpret User Needs, Refine System Performance Specifications & Environmental Constraints

System Safety should:
1. Develop lifecycle environmental profile and system boundaries
2. Develop more detailed system safety criteria
3. Provide input into demilitarization/disposal planning
4. Identify and/or develop system safety-critical requirements (e.g., update the Safety Requirements/Criteria Requirements Analysis [SRCA])
5. Verify system safety-critical requirements are included in requirements tracking system

Develop System Functional Specifications & System Verification Plan

System Safety should:
1. Initiate development of Preliminary Hazard Analysis (PHA)
2. Initiate Threat Hazard Assessment (THA)
3. Update system safety criteria
4. Provide updated input for demilitarization/disposal planning
5. Expand SRCA to include functional specifications
6. Verify system safety-critical functional specifications are included in requirements tracking system
7. Include system safety-critical specifications in System Verification Plan

Evolve Functional Performance Specifications into Configuration Item (CI) Functional (Design to) Specifications and CI Verification Plan

System Safety should:
1. Finalize PHA and initiate development of appropriate Subsystem Hazard Analyses (SSHAs)
2. Finalize THA
3. Update system safety criteria to include test requirements (component, subsystem)
4. Provide updated input for demilitarization/disposal planning
5. Expand and update SRCA as detailed design specifications evolve

System Development and Demonstration Phase

6. Verify system safety-critical design specifications are included in requirements tracking system and detailed design specifications
7. Include system safety-critical specifications in CI Verification Plan

Evolve CI Functional Specifications into Product (Build to) Documentation and Inspection Plan

System Safety should:
1. Finalize SSHAs
2. Initiate development of both System Hazard Analysis (SHA) and Operating and Support Hazard Analysis (O&SHA)
3. Update system safety criteria to include test and inspection requirements (component, subsystem, system)
4. Provide updated input for demilitarization/disposal planning
5. Identify system safety-critical process for product build-to documentation (e.g., safety-critical items list)
6. Include system safety-critical processes and components in inspection plan (e.g., component screening and testing)
7. Participate in component design selections using system safety analyses
8. Expand and update SRCA as necessary
9. Verify system safety-critical design specifications are included in requirements tracking system and detailed design specifications as necessary

Fabricate, Assemble, Code to "Build-to" Documentation

System Safety should:
1. Evaluate process and design changes as necessary
2. Review and recommend updates to TEMP based upon system safety analyses
3. Ensure CI verification Developmental Test & Evaluation (DT&E) procedures include safety requirements and verification testing
4. Initiation safety release documentation, as appropriate

Individual CI Verification Developmental Test & Evaluation (DT&E)

System Safety should:
1. Ensure safety tests were conducted and review test results for hazard control effectiveness
2. Update hazard status
3. Verify integrated DT&E, Live Fire Test & Evaluation (LFT&E) & Early Operational Assessment (EOA) procedures include appropriate tests derived from system safety analyses
4. Recommend hazard closure based on DT&E test results as appropriate
5. Provide safety release documentation, as appropriate

System Development and Demonstration Phase

Integrated DT&E, Live Fire Test & Evaluation (LFT&E) & Early Operational Assessments (EOAs) Verify Performance Compliance to Specifications

System Safety should:

1. Ensure safety tests were conducted and review test results for hazard control effectiveness
2. Update hazard status
3. Update hazard analyses based upon configuration changes
4. Assess configuration changes for test and document results (e.g., safety assessment) as necessary
5. Provide updated input for demilitarization/disposal planning
6. Verify system DT&E, LFT&E & EOA procedures include appropriate tests derived from system safety analyses
7. Recommend hazard closure based on test results
8. Provide safety release for upcoming test activities as appropriate

System DT&E, LFT&E & (Operational Assessments) OAs, Verify System Functionality & Constraints Compliance to Specifications

System Safety should:

1. Ensure safety tests were conducted and review test results for hazard control effectiveness
2. Update hazard status
3. Update hazard analyses based upon configuration changes
4. Assess configuration changes for testing and document results (e.g., safety assessment) as necessary
5. Verify combined DT&E/OA/LFT&E procedures include appropriate tests derived from system safety analyses
6. Recommend hazard closure based on test results, as appropriate
7. Provide safety release for upcoming test activities, as appropriate

Combined DT&E/OT&E/LFT&E Demonstrate System to Specified User Needs & Environmental Constraints

System Safety should:

1. Ensure safety tests were conducted and review test results for hazard control effectiveness
2. Update hazard status
3. Update hazard analyses based upon configuration changes
4. Recommend hazard closure based on test results, as appropriate

System Requirements Review (SRR)

System Safety should present system safety-critical requirements at SRR.

System Functional Review (SFR)

System Safety should present system safety-critical functions at SFR.

Preliminary Design Review (PDR)

System Safety should present PHA and status of hazards at PDR.

Critical Design Review (CDR)

System Safety should present status of hazards in CDR.

System Development and Demonstration Phase

Test Readiness Review (TRR)

System Safety should:
1. Assess configuration for testing and document results (e.g., safety assessment) and present at TRR.
2. Ensure all safety releases are completed in support of TRR

System Verification Review (SVR)

System Safety should present residual risk to user at SVR.

Production Readiness Review (PRR)

System Safety should present system safety-critical requirements at PRR.

Functional Configuration Audit (FCA)

System Safety should review the FCA

Trades

Throughout this phase, System Safety should participate in the trade studies to evaluate options against established system safety criteria.

System Development and Demonstration Phase

Outputs	System Safety Should:
Initial Production Baseline	1. Identify system safety-critical items and processes 2. Identify inspection requirements
Test Reports	1. Verify mitigation controls are effective to reduce risk of hazard 2. Analyze anomalies, incidents, and mishaps
Test and Evaluation Master Plan (TEMP)	1. Update specific test requirements (e.g., MIL-STD-2105C, MIL-STD-1316, MIL-STD-331, MIL-STD-1901, IEEE/EIA 12207, 29CFR1910.9) 2. Include requirements for verification of risk mitigation controls (based upon system safety analyses) 3. Identify safety release requirements, e.g., SAR
Elements of Product Support	Provide the results of the Operating & Support Hazard Analysis (O&SHA)
Risk Assessment	1. Document and report on residual risks and risk acceptance decisions 2. Document concurrence/approval of applicable Service safety boards
Systems Engineering Plan (SEP)	1. Update strategy for integrating ESOH risk management into SE 2. Identify applicable safety boards and process for concurrence/approval
Technology Readiness Assessment	Update the mitigation technology readiness levels (e.g., insensitive munitions technology)
Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE)	1. Update hazard status 2. Update hazard analyses 3. Update ESOH inputs for preliminary demilitarization/disposal plan
Inputs to Capability Production Document (CPD), System Threat Assessment (STA), Integrated Support Plan (ISP), Cost/Manpower Estimate	1. Recommend operational and maintenance training and staffing requirements 2. Update system attrition rate inputs due to mishaps 3. Update hazard mitigation requirements 4. Update insensitive munitions requirements 5. Update mishap reduction requirements

Production and Deployment Phase

Production and Deployment Phase V-Chart
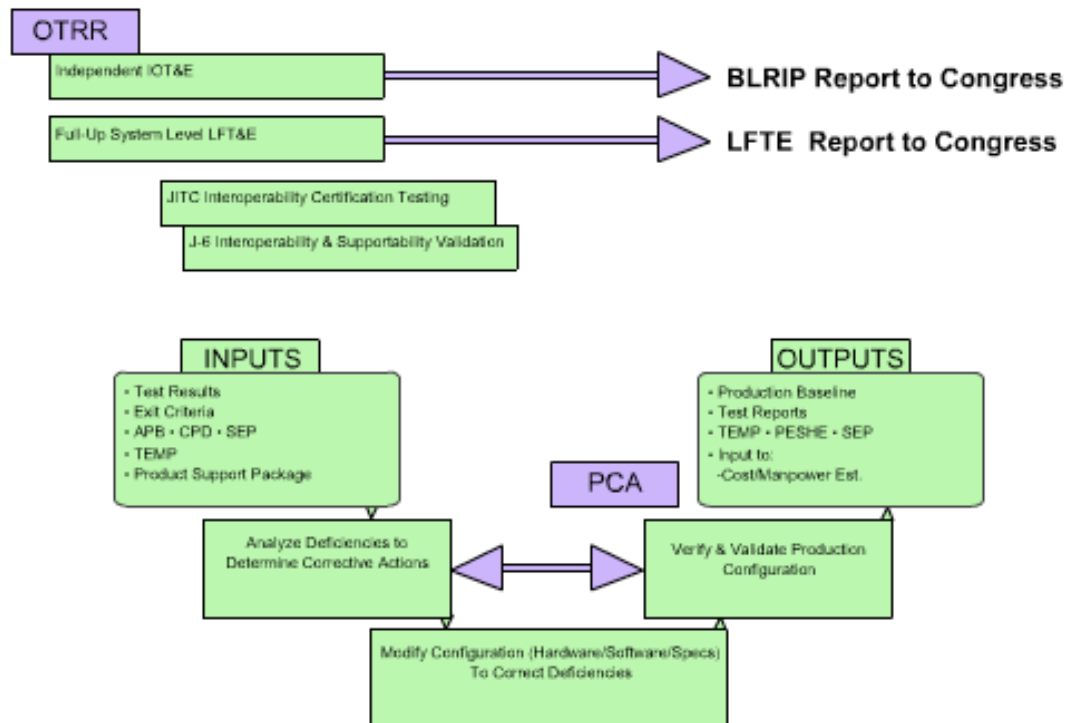
Independent Initial Operational Test and Evaluation (IOT&E) - Beyond Low Rate Initial Production (BLRIP) Report to Congress

Full-Up System Level Live Fire Test and Evaluation (LFT&E) - Live Fire Test and Evaluation (LFTE) Report to Congress

Joint Interoperability Test Command (JITC) Interoperability Certification Testing

J-6 Interoperability and Supportability Validation

Production and Deployment Phase

Inputs	System Safety Should:
Test Results	1. Review Initial Operational Test & Evaluation (IOT&E) results for the effectiveness of risk mitigation controls 2. Analyze anomalies, incidents, and mishaps
Exit Criteria	1. Document formal risk disposition of identified hazards, e.g., Safety Assessment Report (SAR) 2. Obtain concurrence/approval of appropriate safety boards 3. Update Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE) 4. Provide updated inputs for demilitarization/disposal plan
Acquisition Program Baseline	Provide inputs as requested
Capability Production Document (CPD)	1. Update hazard mitigation requirements as necessary 2. Update insensitive munitions requirements as necessary 3. Identify mishap reduction requirements as necessary
Systems Engineering Plan (SEP)	1. Update strategy for integrating ESOH risk management into SE 2. Identify applicable safety boards and process for concurrence/approval
Test and Evaluation Master Plan (TEMP)	1. Update specific test requirements (e.g., MIL-STD-2105C, MIL-STD-1316, MIL-STD-331, MIL-STD-1901, IEEE/EIA 12207, 29CFR1910.95) 2. Update requirements for verification of risk mitigation controls (based upon system safety analyses) 3. Update safety release requirements, e.g., SAR
Product Support Package	Include O&SHA results

Analyze Deficiencies To Determine Corrective Actions

System Safety should:
1. Review deficiency reports for system safety implications
2. Participate in development of corrective actions
3. Participate in Configuration Control Board to include reviewing Engineering Change Proposals (ECPs)

Modify Configuration (Hardware/Software/Specs) To Correct Deficiencies

System Safety should:
1. Identify system safety-critical items and inspection requirements
2. Review and recommend updates to TEMP/test pan based upon system safety analyses
3. Provide safety release documentation as appropriate

Production and Deployment Phase

Verify & Validate Production Configuration
System Safety should:
1. Verify and validate system safety-critical item configuration.
2. Participate in test activities as appropriate

Operational Test Readiness Review (OTRR)
System Safety should update the Safety Assessment Report (SAR) to support the PM's requirement to provide a safety release.

Physical Configuration Audit (PCA)
System Safety should review PCA to identify potential system safety implications.

Outputs	System Safety Should:
Production Baseline	1. Identify system safety-critical items and processes 2. Specify inspection requirements 3. Document concurrence/approvals of applicable safety boards
Test Reports	1. Document effectiveness of risk mitigation controls 2. Document findings from anomalies, incidents, and mishaps
Test and Evaluation Master Plan (TEMP)	1. Update specific test requirements (e.g., MIL-STD-2105C, MIL-STD-1316, MIL-STD-331, MIL-STD-1901, IEEE/EIA 12207, 29CFR1910.95) 2. Update requirements for verification of risk mitigation controls (based upon system safety analyses) 3. Identify safety release requirements, e.g., SAR
Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE)	1. Update hazard status 2. Update hazard analysis 3. Identify applicable safety boards and process concurrence/approval
Systems Engineering Plan (SEP)	1.Update strategy for integrating ESOH risk management into SE 2. Identify applicable safety boards and process concurrence/approval
Input to Cost/Manpower Estimate	1. Recommend training and staffing requirements 2. Update system attrition rate input due to mishaps

Operations and Support Phase

Operations and Support Phase V-Chart
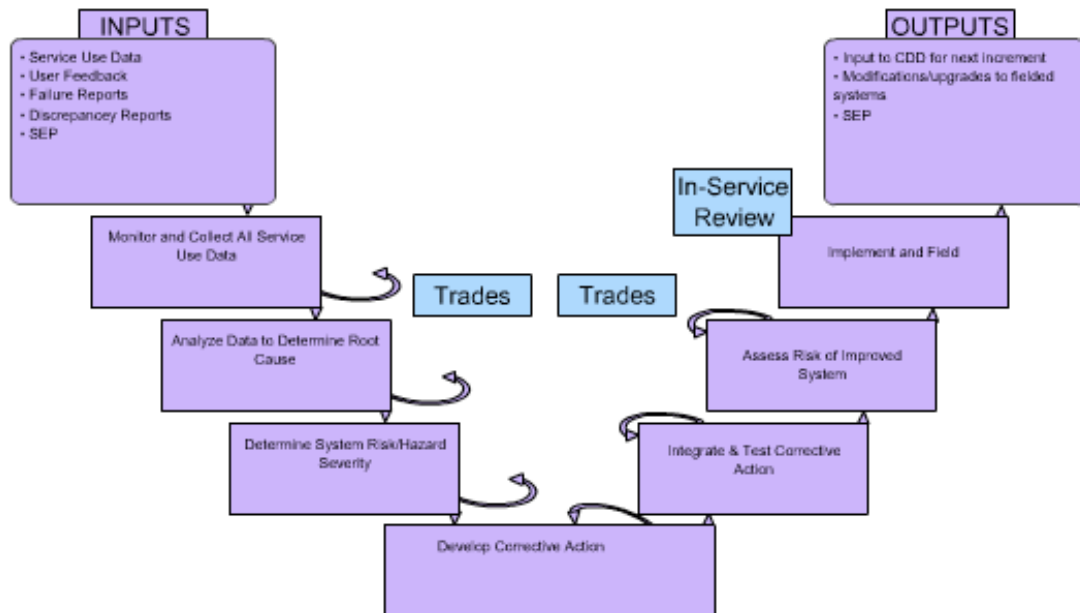
Inputs	System Safety Should:
Service Use Data	Review for system safety implications
User Feedback	Review for system safety implications
Failure Reports	1. Review Follow-On Operational Test & Evaluation (FOT&E) results for system safety implications 2. Review failure/mishap reports for causal factors or mitigation failures and recommend alternative mitigation measures 3. Assist in mishap investigations as requested
Discrepancy Reports	Review discrepancy reports for system safety implications
Systems Engineering Plan (SEP)	1. Update strategy for integrating ESOH risk management into SE 2. Identify applicable safety boards and process for concurrence/approval

Monitor and Collect All Service Use Data
System Safety should:
1. Provide system safety review criteria to engineering and logistics staff
2. Review data for system safety implications (e.g., trend analysis)

Operations and Support Phase

3. Identify opportunities for technology insertion to reduce risk (new technologies, obsolescence)

Analyze Data to Determine Root Cause

System Safety should:
1. Apply appropriate system safety analysis technique to determine root cause (e.g., Failure Modes, Effects, and Criticality Analysis [FMECA], Fault Tree Analysis [FTA])
2. Evaluate data for system safety implications
3. Update hazard analyses/database as appropriate

Determine System Risk/Hazard Severity

System Safety should:
1. Prioritize hazards for risk mitigation
2. Update hazard analyses/database as appropriate

Develop Corrective Action

System Safety should:
1. Apply system safety order of precedence to corrective actions
2. Update hazard analyses/database as appropriate
3. Identify requirements for verification of risk mitigation controls (based upon updated system safety analyses)

Integrate & Test Corrective Action

System Safety should:
1. Evaluate test results for risk mitigation effectiveness
2. Update hazard analyses/database as appropriate

Assess Risk of Improved System

System Safety should:
1. Update hazard analyses/database as appropriate
2. Recommend hazard closure to appropriate risk acceptance authorities (updated residual risk)

Implement and Field

System Safety should continue to track system health, mishaps, hazards, closure actions, mitigation measure effectiveness, and residual risk.

In-Service Review

System Safety should:
1. Provide inputs to the In-Service Review on mishaps
2. Provide inputs to the In-Service Review on any newly identified hazards with assessment of risks, selected mitigation measures, verification of mitigation controls, and acceptance of residual risks

Trades

Throughout this phase, System Safety should participate in the trade studies to evaluate options against established system safety criteria.

Operations and Support Phase

Outputs	System Safety Should:
Input to Capability Development Document (CDD) for next increment	1. Update hazard mitigation requirements as necessary 2. Update insensitive munitions requirements as necessary 3. Update mishap reduction requirements as necessary
Modifications/upgrades to fielded systems	1. Recommend an appropriate funding level for system safety 2. Present updated residual risk to user (e.g., safety assessment) 3. Provide updated inputs for demilitarization/disposal plan
Systems Engineering Plan (SEP)	1. Update strategy for integrating ESOH risk management into SE 2. Identify applicable safety boards and process for concurrence/approval